UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,393	01/27/2006	Junbiao Zhang	PU030228	3745

24498 7590 03/11/2009

Robert D. Shedd
Thomson Licensing LLC
PO Box 5312
PRINCETON, NJ 08543-5312

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
03/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/566,393	ZHANG, JUNBIAO	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/14/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,25-34,36 and 41-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,25-34,36 and 41-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application 10/560,020 filed on 1/27/2006; amendment filed on 1/14/2009.

2. Applicant's arguments, with respect to claims 1-13, 25-34, 36, 41-57 have been fully considered but they are not persuasive.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 48-57** are rejected under 35 U.S.C. 102(b) as being anticipated by Levergood et al. (US 5708780) (hereinafter Levergood).

As per claim 48, Levergood discloses "a method for controlling network access, said method comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "receiving a re-directed request for network access via a message" (column 3, line 27-29, Levergood discloses that content server initiates the authorization routine by redirecting the client's request via URL) "transmitting a client identifier and unique data" (column 5, line 49-65, an SID provided from the authentication server to the client. The SID includes 22-bit user identifier, and

other specific data) "and generating a web page including embedded data" (column 3, line 56-58, when user want to traverse a link to view another web page; line 62-65, the browser generates the new web page by rewriting the current URL to replace the old name, the new URL retains SID).

As per claim 49, Levergood discloses "the method according to claim 48, wherein said unique data comprises a session identifier and a random number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 50, Levergood discloses "the method according to claim 48, wherein said embedded data comprises a session identifier, a random number and authentication server selection information" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as session identifier).

As per claim 51, Levergood discloses "a system for controlling network access, comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "means for receiving a re-directed request for network access via a message" (column 3, line 27-29, Levergood discloses that content server initiates the authorization routine by redirecting the client's request via URL) "means for

transmitting a client identifier and unique data" (column 5, line 49-65, an SID provided from the authentication server to the client. The SID includes 22-bit user identifier, and other specific data) "and means for generating a web page including embedded data" (column 3, line 56-58, when user want to traverse a link to view another web page; line 62-65, the browser generates the new web page by rewriting the current URL to replace the old name, the new URL retains SID).

As per claim 52, Levergood discloses "the system according to claim 51, wherein said unique data comprises a session identifier and a random number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 53, Levergood discloses "the system according to claim 51, wherein said embedded data comprises a session identifier, a random number and authentication server selection information" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as session identifier).

As per claim 54, Levergood discloses "a method for controlling network access, said method comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "receiving an authentication user input

message" (column 6, line 36-41, authentication server receives a request from client) "transmitting authentication input page requesting authentication information" (column 6, line 44-49, sends a challenge response which causes the client browser to prompt the user for credentials. In light of the specification, it discloses "the MT/client responds to the authentication input request by supplying its credentials to the AS 250" (page 7, line 10-11, and fig. 3, 250); sends meaning the transmitting; therefore, Levergood discloses transmitting authentication information to request the credentials to authenticate the user) "receiving authentication credentials; and transmitting an authentication message indicating one of success and failure of an authentication process" (column 6, line 58-66, and column 7, line 1-20, upon receive the request, if the user is not cleared for authorization, a page denying access is transmitted to the client browser. If the user is qualified, the access of the resource is granted).

As per claim 55, Levergood discloses "the method according to claim 54, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number" (column 6, line 5-16, the authentication request get URL contains a SID, and User IP. From line column 54 to 64, Levergood teaches that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. User IP is considered as session identifier. Since the SID is encoded the data it includes a random number).

As per claim 56, Levergood discloses "a system for controlling network access, comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "means for receiving an authentication user input message" (column 6, line 36-41, authentication server receives a request from client) "means for transmitting authentication input page requesting authentication information" (column 6, line 44-49, sends a challenge response which causes the client browser to prompt the user for credentials. In light of the specification, it discloses "the MT/client responds to the authentication input request by supplying its credentials to the AS 250" (page 7, line 10-11, and fig. 3, 250); sends meaning the transmitting; therefore, Levergood discloses transmitting authentication information to request the credentials to authenticate the user) "means for receiving authentication credentials; and means for transmitting an authentication message indicating one of success and failure of an authentication process" (column 6, line 58-66, and column 7, line 1-20, upon receive the request, if the user is not cleared for authorization, a page denying access is transmitted to the client browser. If the user is qualified, the access of the resource is granted).

As per claim 57, Levergood discloses "the system according to claim 56, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number" (column 6, line 5-16, the authentication request get URL contains a SID, and User IP. From line column 54 to 64, Levergood teaches that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. User IP is

considered as session identifier. Since the SID is encoded the data it includes a random number).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-13, 34, 36, and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US 5708780) (hereinafter Levergood) in view of Stewart et al. (US 6732176) (hereinafter Stewart), and further in view of Hinton et al. (WO 02/39237 A2) (hereinafter Hinton).

As per claims 1, Levergood discloses "a method for controlling access to a network, said method comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client;" (column 3, line 8-29, with respect to this limitation, Levergood discloses that client request is received by the internet server which is also called content sever to access controlled files. Examiner considers the internet server is the access point of the network) "re-directing, by said AP, said access request to a local server;" (column 3, line 27-29, Levergood discloses that content server initiates the authorization routine by redirecting the client's request to an authentication server) "transmitting an

authentication request to said selected authentication server" (column 3, line 26-29, with respect to this limitation, Levergood discloses redirecting the client's request to an authentication server) "and receiving a response to said authentication request from said selected authentication server" (column 3, line 29-33, Levergood discloses this limitation by the authentication server returns a response to qualified client).

Levergood does not specifically disclose "associating unique data with an identifier of said client and storing a mapping of said association in said AP" and "generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client".

However, Stewart discloses "associating unique data with an identifier of said client and storing a mapping of said association in said AP" (column 2, line 49-53, and access point associates user identification information to a network provider list. Unique data appears to be the network provider list).

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via a wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request of Levergood at an access point or an computing device as described in Stewart because it would provide for varying the options to be authenticated to a network.

Furthermore, Hinton discloses "generating a web page by said local server requesting that said client select an authentication server (AS) and including said

unique data and forwarding said generated Web page to said client" (page 23, line 17-34, and page 24, line 1-3, server generates a web page for client to select all the available servers/services (including authentication service). Server 404 sends HTTP redirects to the client including introductory authentication token. Figure 4A discloses the token includes user ID which considers equal meaning with unique data. Figure 3B depicts an exemplary webpage).

Levergood and Stewart, and Hinton are analogous art because they all attempt to satisfy the different authentication needs when come to access a network or the Internet.

It would have been obvious to one of ordinary skilled in the art at the time of invention to generate a web page for user to select the next website that client desire to locate by clicking on the link as described by Hinton to facilitate the service providers list that client needs to choose that depicts by Levergood in view of Stewart because it would provide to use a web page for communication between a client and a server is easier implement in technical point and more explicit/user friendly to client to make the select.

As per claim 2, Hinton discloses "the method according to claim 1, wherein said network is a wireless Local Area network (WLAN)" (page 10, line 12-20, the network 101 may include permanent connections, such as wire or fiber optic cables, or connections made through wireless communications).

As per claim 3, Levergood discloses "the method according to claim 1, further comprising: forwarding said identifier of said client from said local server; and

generating said unique data for said client by said local server" (column 3, line 24-26, the internet server subjects the client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server).

As per claim 4, Levergood discloses "the method according to claim 1, further comprising: retrieving, by said client, a re-directed URL having embedded data including a first digital signature, authentication parameters and said unique data and forwarding said re-directed URL to said AP" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as said identifier. The browser forwards the request to a content server 120. As stated above, content server is considered as AP) "creating, by said AP, a second digital signature using said authentication parameters, said unique data and said identifier; comparing, by said AP, said first digital signature with said second digital signature" (column 6, line 5-8, the content server which is considered as AP tagged with SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16 character ASCII string is considered as said unique data, and the authorized IP address is considered as said identifier. The browser forwards the request to a content

server 120) "determining, by said AP, if there is a match between said first digital signature and said second digital signature" (column 6, line 8-16, the SID's digital signature is compared against the digital signature computed) "and performing, by said AP, one of granting network access and denying network access based on said match determination" (column 6, line 17-20, with respect to this limitation, Levergood discloses if the validation passes, the controlled resources will be granted to access).

As per claim 5, Levergood discloses "the method according to claim 1, wherein said unique data includes a session ID and a randomized number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 6, Levergood discloses "the method according to claim 1, wherein said identifier is an address of said client" (column 5, line 61-65, the authorized IP address is considered as said identifier of the user).

As per claim 7, Levergood discloses "the method according to claim 1, wherein the act of authenticating further comprises: processing, by said AS, said authentication request, wherein said authentication request includes a session ID embedded in said authentication request" (column 6, line 27-65, client browser automatically sends a GET request to authentication server. Levergood discloses the embedded session ID in line 62-63 by such as client IP address and password, as well as other information) "responding to said authentication request by forwarding to said client by said AS an authentication input page, said authentication input page including a request for authentication information" (column 6, line 40-49, with respect to this limitation,

Levergood discloses authentication server sends a challenge responds which causes the client browser to prompt the user for credentials) "and receiving, by said AS, authentication credentials from said client, wherein said response to said authentication request forwarded to said client includes a re-direct header and a success code and associated information relevant to access of said network by said client" (column 6, line 58-67, and column 7, line 1-21, Levergood discloses this limitation by if user is authorized, the authentication server transmits a redirect response based on the tagged URL to client browser. An SID for an authorized user is appended).

As per claim 8, Levergood discloses "the method according to claim 7, wherein the act of forwarding further comprises generating, by said AS, said success code and said associated information includes a first digital signature and authentication parameters" (column 7, line 14-20, an SID for an authorized user is appended. Levergood discloses The SID is sixteen character ASCII string and it contains a 32-bit digital signature in column 5, line 54-61. It is the as same as the SID Levergood mentioned in the rejection of claim 4).

As per claim 9, Levergood discloses "the method according to claim 5, wherein said randomized number is one of a random number and a pseudo-random number" (column 5, line 54-65, the sixteen character ASCII string that encodes 96 bits of SID data. Since the SID is encoded the data it includes a random number or pseudo-random number).

As per claim 10, Levergood and Steward disclose "the method according to claim 1, wherein said identifier is one of a physical (PHY) address of said client, a MAC

address of said client and an IP address of said client" (in column 5, line 54-65, Levergood discloses "an IP address of said client" by the SID which has the equal meaning of identifier contains a 32-bit digital signature, and the digital signature includes the IP address of the user. In column 2, line 34-39, Stewart discloses "a MAC address of said user" by the identification information may take various forms, such as system ID, MAC ID etc).

As per claim 11, Steward discloses "the method according to claim 1, wherein said AP and said local server are co-located" (column 2, line 63-66, the memory medium which may be a computer system can be comprised in the access point).

As per claim12, Levergood discloses "the method according to claim 4, wherein said first and said second digital signatures are generated using one of a private key of said AS and a shared key between said AS and said local server" (column 5, line 61-65, the digital signature is a cryptographic hash that encrypted with secret key which is shared by the authentication and content servers).

As per claim 13, Levergood discloses "the method according to claim 4, wherein said second digital signature is locally generated at said AP" (column 6, line 5-13, the first digital signature is compared against the second digital signature that computed by content server).

As per claim 34, Levergood discloses "the method of claim 1, further comprising: at the authentication server, authenticating the client using the unique data, and forwarding said response to the client using a re-direct header, and including a digitally signed authentication message and authentication parameters corresponding to the

unique data (column 7, line 14-20, an SID for an authorized user is appended. The authentication server then transmits a redirect response to the client browser. Levergood discloses the SID is sixteen characters ASCII string and it contains a 32-bit digital signature, a 2-bit expiration date, a 22-bit user identifier and other information included in column 5, line 54-61) "and the access point receiving from the client according to the re-direct header the digitally signed authentication message and authentication parameters" (column 7, line 14-20, content server receiving from the user according to the original URL directed header with an SID for the user is appended. Levergood discloses the SID is sixteen characters ASCII string and it contains a 22-bit user identifier and other information included in column 5, line 54-61).

Stewart discloses "correlating the authentication parameters with the mapped association data for determining access to the network" (column 2, line 60-67, and column 3, line 1-6, compare the received parameters with the mapped corresponding list to determine the appropriate network provider to access).

AS per claim 36, Levergood discloses "the method of claim 1, wherein said unique data comprises a session ID and a randomized number and further comprising: receiving, by said AP, a re-directed request from the client and including a digitally signed authentication message, an authentication parameter list, and said session ID, the digitally signed authentication message being generated using the randomized number, said session ID and said authentication parameter list, by said selected authentication server associated with the client" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID to content server. From line 54 to

64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. Since it is encoded it is involved in a randomized number. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The URL directed to is the selected authentication server to the user). Steward discloses "and correlating the received digitally signed authentication message with the re-directed request for access using the stored mapping data for controlling access by the client to the network" (column 2, line 49-66, access point receives the identification information for using a stored list to map for the controlling network access).

As per claim 41, Steward discloses "the method according to claim 36, wherein said AP and said LS are co-located" (column 2, line 63-66, the memory medium which may be a computer system can be comprised in the access point).

As per claim 26, Levergood discloses "a system for controlling access to a network comprising: a client; an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client" (column 3, line 7-29, and figure3, the invention related to methods of processing service requests from a client to a server through a network, it includes, a client, a internet server, and a content server. Content server serves the same function as an AP, and internet server servers the same function as a local server) "and an authentication server for performing an authentication process in response to a request from the client" (column 3, line 29-34, an authentication returns a response to interrogate the client and issue certificate to client) "the LS transmits the unique data to the client" (column 3, line 26-29, Levergood

discloses redirecting the client's request to an authentication server, and the server subjects the client to client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server) "the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data" (column 7, line 14-20, an SID for an authorized user is appended. The authentication server then transmits a redirect response to the client browser. Levergood discloses the SID is sixteen characters ASCII string and it contains a 32-bit digital signature, a 2-bit expiration date, a 22-bit user identifier and other information included in column 5, line 54-61) "the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client" (column 7, line 14-20, content server receiving from the user according to the original URL directed header with an SID for the user is appended. Levergood discloses the SID is sixteen characters ASCII string and it contains a 22-bit user identifier and other information included in column 5, line 54-61).

Levergood does not specifically disclose "wherein the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association" and "the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation".

However, Stewart discloses "wherein the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association" (column 2, line 42-66, access point detect identification information, and later discloses to store a list of identification information that maps to a corresponding list) "and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation" (column 2, line 60-67, and column 3, line 1-6, compare the received parameters with the mapped corresponding list to determine the appropriate network provider to access).

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request of Levergood at an access point or an computing device as described in Stewart because it would provide for varying the options to be authenticated to a network.

Furthermore, Hinton discloses "the system of claim 25, wherein the network is a wireless local area network (WLAN) comprising the access point and local server" (page 10, line 12-20, the network 101 may include permanent connections, such as wire or fiber optic cables, or connections made through wireless communications). Levergood discloses "comprising the access point and local server" (column 3, line 7-29, the invention includes, a client, an internet server, and a content server. Content server

serves the same function as an AP, and internet server servers the same function as a local server).

Levergood and Stewart, and Hinton are analogous art because they all attempt to satisfy the different authentication needs when come to access a network or the Internet.

It would have been obvious to one of ordinary skilled in the art at the time of invention to generate a web page for user to select the next website that client desire to locate by clicking on the link as described by Hinton to facilitate the service providers list that client needs to choose that depicts by Levergood in view of Stewart because it would provide to use a web page for communication between a client and a server is easier implement in technical point and more explicit/user friendly to client to make the select.

As per claim 33, Steward discloses "the system of claim 26, wherein said AP and said LS are co-located" (column 2, line 63-66, the memory medium which may be a computer system can be comprised in the access point).

5. Claims 25, 27-32, and 42-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US 5708780) (hereinafter Levergood) in view of Stewart et al. (US 6732176) (hereinafter Stewart).

As per claim 25, Levergood discloses "a system for controlling access to a network comprising: a client; an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client" (column 3, line 7-29, and figure3, the invention related to methods of processing service requests from a client to

a server through a network, it includes, a client, a internet server, and a content server. Content server serves the same function as an AP, and internet server servers the same function as a local server) "and an authentication server for performing an authentication process in response to a request from the client" (column 3, line 29-34, an authentication returns a response to interrogate the client and issue certificate to client) "the LS transmits the unique data to the client" (column 3, line 26-29, Levergood discloses redirecting the client's request to an authentication server, and the server subjects the client to client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server) "the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data" (column 7, line 14-20, an SID for an authorized user is appended. The authentication server then transmits a redirect response to the client browser. Levergood discloses the SID is sixteen characters ASCII string and it contains a 32-bit digital signature, a 2-bit expiration date, a 22-bit user identifier and other information included in column 5, line 54-61) "the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client" (column 7, line 14-20, content server receiving from the user according to the original URL directed header with an SID for the user is appended. Levergood discloses the SID is sixteen characters ASCII string and it contains a 22-bit user identifier and other information included in column 5, line 54-61).

Levergood does not specifically disclose "wherein the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association" and "the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation".

However, Stewart discloses "wherein the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association" (column 2, line 42-66, access point detects identification information, and stores a list of identification information that maps to a corresponding list; column 11, line 17-27, on top of user transmits the identification information described before , Stewart also discloses that user submits additional geographic location information to AP, AP redirect the information to a network provider, after network provider acknowledges the user's geographic location, AP in response to the redirected request to access to network provider from the user, then redirect the information from provider to user) "and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation" (column 2, line 60-67, and column 3, line 1-6, compare the received parameters with the mapped corresponding list to determine the appropriate network provider to access).

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request of Levergood at an access point or an computing device as described in Stewart because it would provide for varying the options to be authenticated to a network.

As per claim 27, Levergood discloses "the system of claim 25, wherein the local server generates a web page requesting that the client select an authentication server, and embeds the unique data in the web page for transmission to the client" (column 3, line 24-26, the internet server subjects the client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server).

As per claim 28, Levergood and Steward disclose "the system of claim 25, wherein the identifier of the client is one of a physical address, MAC address and an IP address" (in column 5, line 54-65, Levergood discloses "an IP address of said client" by the SID which has the equal meaning of identifier contains a 32-bit digital signature, and the digital signature includes the IP address of the user. In column 2, line 34-39, Stewart discloses "a MAC address of said user" by the identification information may take various forms, such as system ID, MAC ID etc.). Levergood discloses "and wherein the unique data comprises a session ID and a randomized number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 29, Levergood discloses "the system of claim 28, wherein the session ID and randomized number are generated by the local server" (column 3, line

24-26, the internet server subjects the client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server. According to column 5, line 54-65, the SID is a sixteen character ASCII string that encodes 96 bits of SID data. Since the SID is encoded the data includes a random number).

As per claim 30, Levergood discloses "the system of claim 28, wherein the authentication server receives user credential information from the client and provides a digitally signed authentication message including an authentication parameters using said unique data through HTTPS to the client via said re-direct header to the client" (column 6, line 42-49 and column 7, line 14-19, authentication server send challenge response and receives user credential, and issue an appropriate SID. It includes digitally signed authentication message for authorize user, and redirect response on the tagged URL to client browser).

As per claim 31, Levergood and Stewart disclose "the system of claim 30, wherein the AP, in response to receiving the digitally signed authentication message re-directed from the client including the authentication parameters and at least a portion of the unique data from the client" (column 7, line 14-20, Levergood discloses that content server receiving from the user according to the original URL directed header with an SID for the user is appended. Levergood discloses the SID is sixteen characters ASCII string and it contains a 22-bit user identifier and other information included in column 5, line 54-61) "generates a local digital signature using the received portion of the unique data and compares the local digital signature with the digitally signed authentication

message to determine network access by the client" (column 6, line 8-16, with respect to this limitation, Levergood discloses that the SID's digital signature is compared against the digital signature computed from the remaining item of the SID. If the validation passes, the access is authorized) "and the stored mapping data together with the authentication parameters" (column 2, line 60-63, Stewart discloses stores a list of identification information that maps to a corresponding list).

As per claim 32, Levergood discloses "the system of claim 25, wherein the re-direct header further comprises a means for re-directing a browser of the client to a URL on the network, and embedding in the URL said digitally signed authentication message, the authentication parameters and a portion of the unique data (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as said identifier. The browser forwards the request to a content server 120. As stated above, content server is considered as AP.).

As per claim 42, Levergood discloses "a method for controlling network access, said method comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "receiving a request for network access" (column 3, line 7-89, process service requests form a client to a server) "re-directing said request via a message" (column 3, line 27-29, Levergood discloses that content

server initiates the authorization routine by redirecting the client's request via URL) "receiving a client identifier and unique data" (column 3, line 43-47, receives a URL request accompanied by an SID. The SID includes client identifier and unique data) "receiving a re-directed universal resource locator included embedded information (column 3, line 43-47, receives a URL request accompanied by an SID) "generating a local digital signature using said embedded information and said association between said unique data and said client identifier" (column 5, line 54 to 64, Levergood discloses that the preferred SID includes a 32-bit digital signature that has a 16-bit expiration date, a 2-bit key identifier, and a 22-bit user identifier etc. Therefore, the digital signature using the embedded information of unique data and 22 –bit user identifier) "comparing said local digital signature with a digital signature received in said embedded information" (column 6, line 8-16, the received SID's digital signature is compared against the digital signature computed locally); granting network access if said local digital signature matches said digital signature received in said embedded information; and deny network access if said local digital signature does not match said digital signature received in said embedded information" (column 6, line 17-20, with respect to this limitation, Levergood discloses if the validation passes, the controlled resources will be granted to access. In other words, if the validation does not pass, the controlled resources will not be granted to access).

Levergood does not specifically disclose "associating said unique data and said client identifier".

However, Steward discloses "associating said unique data and said client identifier" (column 2, line 42-66, access point detect identification information, and later discloses to store a list of identification information that maps to a corresponding list).

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request of Levergood at an access point or an computing device as described in Stewart because it would provide for varying the options to be authenticated to a network.

As per claim 43, Levergood discloses "the method according to claim 42, wherein said unique data comprises a session identifier and a random number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 44, Levergood discloses "the method according to claim 42, wherein said embedded information further comprises a session identifier and authentication parameters" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as session identifier).

As per claim 45, Levergood discloses "a system for controlling network access, comprising:" (column 3, line 8-9, methods of processing service requests from a client to a server through a network) "means for receiving a request for network access" (column 3, line 21-29, a client request of access a network is made) "means for re-directing said request via a message" (column 3, line 27-29, Levergood discloses that content server initiates the authorization routine by redirecting the client's request via URL) "means for receiving a client identifier and unique data" (column 3, line 43-47, receives a URL request accompanied by an SID. The SID includes client identifier and unique data) "means for receiving a re-directed universal resource locator included embedded information (column 3, line 43-47, receives a URL request accompanied by an SID) "means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier" (column 5, line 54 to 64, Levergood discloses that the preferred SID includes a 32-bit digital signature that has a 16-bit expiration date, a 2-bit key identifier, and a 22-bit user identifier etc. Therefore, the digital signature using the embedded information of unique data and 22 – bit user identifier) "means for comparing said local digital signature with a digital signature received in said embedded information" (column 6, line 8-16, the received SID's digital signature is compared against the digital signature computed locally); "means for granting network access if said local digital signature matches said digital signature received in said embedded information; and means for deny network access if said local digital signature does not match said digital signature received in said embedded information" (column 6, line 17-20, with respect to this limitation, Levergood

discloses if the validation passes, the controlled resources will be granted to access. In other words, if the validation does not pass, the controlled resources will not be granted to access).

Levergood does not specifically disclose "means for associating said unique data and said client identifier".

However, Steward discloses "means for associating said unique data and said client identifier" (column 2, line 42-66, access point detect identification information, and later discloses to store a list of identification information that maps to a corresponding list).

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request of Levergood at an access point or an computing device as described in Stewart because it would provide for varying the options to be authenticated to a network.

As per claim 46, Levergood discloses "the system according to claim 45, wherein said unique data comprises a session identifier and a random number" (column 5, line 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number).

As per claim 47, Levergood discloses "the system according to claim 45, wherein said embedded information further comprises a session identifier and authentication parameters" (column 5, line 22-65, user redirects URL get request at 100 in Fig. 2A

contains an SID. From line 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as session identifier).

Response to Arguments

8. The request paper submitting under 35 U.S.C. 119(a)-(d) is withdrawn.

9. On page 4 of the applicant's response, the Applicants argue that Levergood does not show or suggest "generating a web page including embedded data" in claim 48 nor "means for generating a web page including embedded data" in claim 51. Please refer to the rejections in the underlined section in claims 48 and 51.

10. On page 5, the Applicants argue that Levergood does not show or suggest "transmitting authentication input page requesting authentication information" and rather "discusses a procedure for checking credentials" in claim 54, and "means for transmitting authentication input page requesting authentication information" in claim 56. In light of the specification, "the MT/client responds to the authentication input request by supplying its credentials to the AS 250" (page 7, line 10-11, and fig. 3, 250); and Levergood discloses the limitation by "sends a challenge response which causes the client browser to prompt the user for credentials" (column 6, line 44-49). "Sends" is to transmit; therefore, Levergood discloses transmitting authentication information to

request the credentials to authenticate the user. Please also refer to the rejection in the underlined sections in claim 54 and 56.

11. On page 6, lines 1-3, the Applicants argue "Levergood does not control access to a network". Lever good discloses it at the first sentence in abstract as "this invention relates to methods for controlling and monitoring access to network servers". Also Levergood discloses control access to a network in Fig. 20A, 106, "the content server determines whether the request is directed to a page within current domain" (col.5, line 66-67, and col. 6, line 1); and in Fig. 2B, 210-212, "whenever the content server redirects the client to the authentication server 200, the authentication server initiates the authorization process by validating that it is for an approved content server and determining the level of authentication required for the access requested 210" (col. 6, line 36-40); therefore, Levergood includes "control of access to file with in a network" in the disclosure, however, it is only one aspect of "access to a network".

12. On page 6, lines 7-11, the Applicants argue that "nowhere Stewart et al show or suggest associating said unique data and said client identifier". Please refer to the rejection in the underlined section in claim 1.

13. On page 6, lines 11-17, the Applicants argue that "nowhere Hinton et al show or suggest generating a web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client, and rather to generate a hyperlink". Please refer to rejection in the corresponding underlined section in claim 1.

14. On page 6, lines 2-1 from bottom and to page 7, line 1-2, the applicants argue that "nowhere Levergood et al show or suggest a system for controlling access to a network, and rather Levergood shows only controls access to a file within a network". Please refer to paragraph 11 above the disclosure from Levergood. Further more, "a system for controlling access to a network" describes the intended use. The purpose or intended use of the invention, rather than any distinct definition of any of the claimed invention's limitations, then the preamble is not considered a limitation and is of no significance to claim construction. Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165 (Fed. Cir. 1999). See also Rowe v. Dror, 112 F.3d 473, 478, 42 USPQ2d 1550, 1553 (Fed. Cir. 1997) ("where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention, the preamble is not a claim limitation").

15. On page 7, lines 2-8, the Applicants argue that "Stewart et al shows or suggests the AP, in response to a redirected request to access the network from client, associates unique data with an identifier of the client and stores a mapping of the association, and rather in Stewart et al, the AP listens for identification information or broadcasts requests for identification information". Please refer to rejection in the underlined section in claim 25.

16. On page 7, lines 14-18, the Applicants argue that "Levergood et al does not control network access, and rather only controls access to a file within a network". Please refer to paragraph 11 above. The Applicants also argue "Levergood et al does not receive a request for network access, rather a request for access to a file within a

network". Please see the rejection in corresponding underlined section in claim 42. Also the service requests are not only to access a file but also to access a network. Please refer to the above paragraph 11.

17. On page 7, lines 5-1 from the bottom, the Applications argue "nowhere Levergood et al show or suggest means for granting network access...and means to deny network access". Please refer to paragraph 11 above for granting network access. Levergood discloses "means to deny network access" (col. 5, lines 66-67, and col. 6, lines 1-4, content server determines whether the request is directed to a page within the current domain, if it is not, the user is redirected to the authentication server, in the other words, the access request has been denied).

18. On page 8, the Applicants cannot agree Levergood and Stewart are analogous art because Levergood does not teach access control to a network, but rather only shows access control of a file within a network. Please refer to paragraph 11 above for the disclosure of the access control to network from Levergood.

Conclusion

19. **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jing Sims

/J. S./

Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437